## C. REMARKS

### Status of the Claims

Claims 1, 6-8, 13-14, 19-20, and 21-29 are currently present in the Application, and claims 1, 8, and 14 are independent claims. Claims 1, 6-8, and 14 have been amended, claims 2-5, 9-12, and 15-18 have been cancelled, and claims 21-29 have been added.

### Examiner Interview

Applicants note with appreciation the telephonic interview conducted between Applicants' representative and the Examiner on November 15, 2005. During the telephonic interview, the Examiner and Applicants' representative discussed the 103 references (Al-Salqan, U.S. Patent No. 6,549,626 and Hosokawa, U.S. Patent Pub. 2001/0023416). In particular, Applicants' representative discussed that Applicants' invention provides a password from a software application to a hardware security module which, in turn, generates an encrypted tied key and returns the encrypted tied key to the software application. The encrypted tied key includes a generated key (first key) that is encrypted using a key that is associated with the hardware security module (second key).

Applicants' representative contended that the 103 references do not teach Applicants' determination steps found in claims 4 and 5, and suggested amending the independent claims to include the limitations of original claims 2-5 in order for the independent claims to read over the art of record. The Examiner wished to review the Applicants' written response before commenting as to whether the amendments read over the art of record.

## Drawings

Applicants note that the Examiner did not indicate whether the formal drawings, filed with Applicants' application, are accepted by the Examiner. Applicants respectfully request that the Examiner indicate whether the formal drawings are accepted in the next office communication.

## Claim Rejections - 35 U.S.C. § 101

Claims 1-8 stand rejected under 35 U.S.C. § 101 because the Office Action alleges that the claimed invention is directed to non-statutory subject matter. Applicants respectfully traverse the rejections. Claims 2-5 have been canceled and, therefore, the 101 rejection to these claims is moot.

The Office Action states "claims 1-8 are non-statutory as all of the claimed features can be implemented in software alone. Thus, these claims are rejected as not being tangible." Applicants respectfully disagree with this statement. Regarding the portion of the statement "these claims are rejected as not being tangible," Applicants would like to draw the Examiner's attention to the Manual of Patent Examining Procedure § 2106, part IV.B, which states in part (emphasis added):

> "A claim that requires one or more acts to be performed defines a process... For such subject matter to be statutory, the claimed process must be limited to a practical application of the abstract idea or mathematical algorithm in the technological arts... A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result..."

Per the MPEP, claims themselves do not have to be tangible but, rather, the claims must produce a concrete, tangible and useful result. Applicants' claim 1 encrypts a key using a password, recovers the key using the same password, and encrypts

data using the recovered password, which is a concrete, tangible and useful result. Claims 6-7 depend upon claim 1 and, therefore, produce a concrete, tangible and useful result as well.

Regarding the portion of the statement "claims 1-8 are non-statutory as all of the claimed features can be implemented in software alone," Applicants would like to point out that software has been patentable for many years because software is capable of implementing a process that, if it produces a concrete, tangible and useful result, is statutory (per MPEP above). In an effort to ensure that the claims are within the technological arts, and in the interest of advancing prosecution of the present Application, Applicants have amended claims 1, 6, and 7. Claims 1, 6, and 7 have been amended to include "***a computer-implemented method*** for securing data," as well as other computer-related phrases as applicable to the claim limitations

MPEP § 2106, part II.A, states in part (emphasis added):

> "A process that consists solely of the manipulation of an abstract idea is not concrete or tangible. See *In re Warmerdam*, 33 F.3d 1354, 1360, 31 USPQ2d 1754, 1759 (Fed. Cir. 1994). See also *Schrader*, 22 F.3d at 295, 30 USPQ2d at 1459. Office personnel have the burden to establish a *prima facie* case that the claimed invention as a whole is directed to solely an abstract idea or to manipulation of abstract ideas or does not produce a useful result. ***Only when the claim is devoid of any limitation to a practical application in the technological arts should it be rejected under 35 U.S.C. 101.*** Compare *Musgrave*, 431 F.2d at 893, 167 USPQ at 289; *In re Foster*, 438 F.2d 1011, 1013, 169 USPQ 99, 101 (CCPA 1971). Further, when such a rejection is made, Office personnel must expressly state how the language of the claims has been interpreted to support the rejection."

With the amendments to claims 1, 6, and 7, these claims cannot be said to be "devoid of any limitation to a practical application in the technological arts." Therefore, Applicants' claims 1, 6, and 7 should not be rejected under 35 U.S.C. § 101, and Applicants respectfully request that the rejections to these claims under 35 U.S.C. § 101 be withdrawn.

Regarding claim 8, claim 8 includes limitations of:

- one or more processors;
- a memory accessible by the processors;
- one or more nonvolatile storage devices accessible by the processors;
- a hardware security module accessible by the processors

The above limitations correspond to computer hardware devices, which clearly cannot be implemented in software alone as suggested by the Office Action. In addition, claim 8 includes limitations similar to claim 1 that produce a concrete, tangible and useful result. Therefore, Applicants' claim 8 should not be rejected under 35 U.S.C. § 101, and Applicants respectfully request that the rejection to claim 8 under 35 U.S.C. § 101 be withdrawn.

**Claim Rejections - Alleged Obviousness Under 35 U.S.C. § 103**

Claims 1-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Al-Salqan (U.S. Patent No. 6,549,626, hereinafter "Al-Salqan") in view of Hosokawa (U.S. Patent Pub. 2001/0023416, hereinafter "Hosokawa"). Applicants respectfully traverse these rejections. Claims 2-5, 9-12, and 15-18 have been canceled and, therefore, the 103 rejection to these claims is moot.

As discussed with the Examiner, Applicants have amended the independent claims to include the limitations of original claims

2-5. As amended, Applicants' independent claims 1, 8, and 14 include the limitations of:

- receiving, at a security module, a first password corresponding to a software application;
- generating, at the security module, a first mask value based on the first password;
- combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
- encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;
- returning the encrypted tied key to the software application;
- determining, at the software application, that the encrypted tied key corresponds to the security module;
- in response to the determining, sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password;
- receiving, at the security module, the encrypted tied key and the second password from the software application;
- in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second key, the combining resulting in a recovered tied key;
- generating a second mask value based on the second password;
- separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and

- encrypting data provided by the software application using the recovered generated key.

Applicants use a security module to encrypt and decrypt data retrieved from a software module. Before the software application provides the data, the software application must first possess an encrypted tied key that corresponds to the software module. Claim 1's first through fifth elements claim the software application providing a first password to the security module and, in turn, the security module providing the encrypted tied key, which has been encrypted with a second encryption key that is associated with the security module, to the software application. Then, in claim 1's sixth element, the software application determines that the encrypted tied key corresponds to the security module, and proceeds to send the encrypted tied key and the password back to the security module in order for the security module to extract a recovered generated key, and encrypt data from the software application using the recovered generated key (seventh through twelfth elements).

Al-Salqan never teaches or suggests interaction between a software application and a security module, but rather teaches interaction between a user and a security module. Therefore, Al-Salqan never teaches or suggests many of Applicants' claim 1 limitations.

First, Applicants claim "receiving, at security module, a first password corresponding to a software application." Al-Salqan's passwords do not correspond to a software application. Rather, Al-Salqan uses "private information" as a password, and states:

> "Private information is information that would likely be know only by the [user] of the key

> received at input 206, such as [a] social security number, mother's maiden name, and other similar information." (col. 4, lines 4-7, emphasis added)

As can be seen, Al-Salqan never teaches or suggest "receiving, at security module, a first password corresponding to a software application" as claimed by Applicants. The Office Action does not contend that Hosokawa teaches such limitation, and indeed Hosokawa does not.

Second, Applicants claim "returning the encrypted tied key to the software application" and "determining, at the software application, that the encrypted tied key corresponds to the security module." This is due to the fact that if the software application has not received the encrypted tied key, the software application is required to request the encrypted tied key from the security module. As discussed above, Al-Salqan never teaches a software application interacting with the security module, let alone a software application managing encrypted tied keys and performing the determining step as claimed by Applicants. Rather, Al-Salqan states:

> "Asymmetric encryptor 242 passes the resulting encrypted key, referred to as a key recovery file, to key recovery file storage 244. Key recovery file storage 244 provides at output 246 the key recovery file, which may be stored by the principal or others to retrieve the key encrypted therein." (col. 4, ln. 67 - col. 5, ln. 5)

As can be seen from the above excerpt, Al-Salqan teaches passing the encrypted key to a storage area or to a user for storage elsewhere. As such, Al-Salqan never teaches or suggests a software application "determining that the encrypted tied key corresponds to the security module" as claimed by Applicants.

The Office Action does not contend that Hosokawa teaches such limitation, and indeed Hosokawa does not.

Third, Applicants claim "encrypting data provided by the software application using the recovered generated key." Since Applicants' claim 1 should be viewed as a whole, the software application provides passwords, receives the encrypted tied key, and provides data to be encrypted by the security module. Al-Salqan never teaches or suggests a software application performing these limitations while interacting with the security module as claimed by Applicants. The Office Action does not contend that Hosokawa teaches such limitations, and indeed Hosokawa does not.

Therefore, since neither Al-Salqan nor Hosokawa teach or suggest, either alone or in combination with each other, all the limitations included in Applicants' claim 1 as amended, claim 1 is allowable over Al-Salqan in view of Hosokawa.

Claim 8 is an information handling system claim including similar limitations of claim 1 and, therefore, is allowable for the same reasons as claim 1. Claim 14 is a computer program product claim including similar limitations of claim 1 and, therefore, is allowable for the same reasons as claim 1.

Each of the remaining claims 6-7, 13, and 19-20 each depend, directly or indirectly, upon one of the allowable independent claims 1, 8, and 14. Therefore, claims 6-7, 13, and 19-20 are each allowable for the same reasons as their respective independent claims.

**New Claims**

Claims 21-23 have been added, which are method claims that are dependent upon claim 1. Claim 21 is allowable over the art

of record because it claims a separate hardware security module performing the key encryption and data encryption limitations of claim 1, whereas the art of record never teaches or suggests a separate hardware security module. Claim 22 is allowable over the art of record because it claims that the generated key is at a security level corresponding to a data sensitivity level, whereas the art of record never teaches or suggests such distinction. Claim 23 is allowable over the art of record because it claims data encryption within the security module, whereas the art of record never teaches or suggests encrypting data within the security module.

Claims 24-26 are information handling system claims including the same limitations as claims 21-23, respectively. Therefore, claims 24-26 are allowable for the same reasons as claims 21-23 are allowable. Claims 27-29 are computer program product claims including the same limitations as claims 21-23, respectively. Therefore, claims 27-29 are allowable for the same reasons as claims 21-23 are allowable.

## Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes

that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By _____

Leslie A. Van Leeuwen, Reg. No. 42,196
Van Leeuwen & Van Leeuwen
Attorney for Applicants
Telephone: (512) 301-6738
Facsimile: (512) 301-6742







BEST AVAILABLE COPY